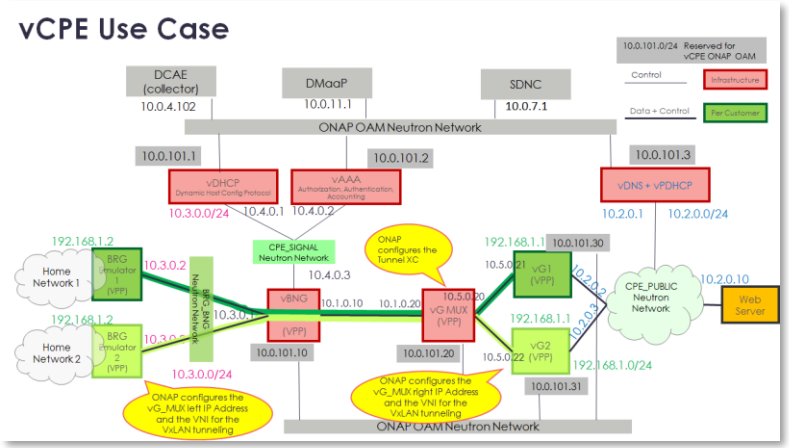
PNF and Hybrid Services Support in ONAP

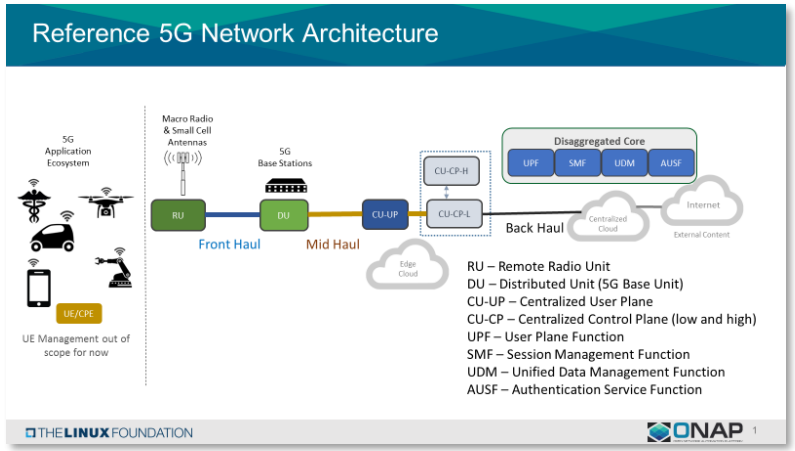
Oskar Malm, Ericsson

v1.1, January 2018

Introduction

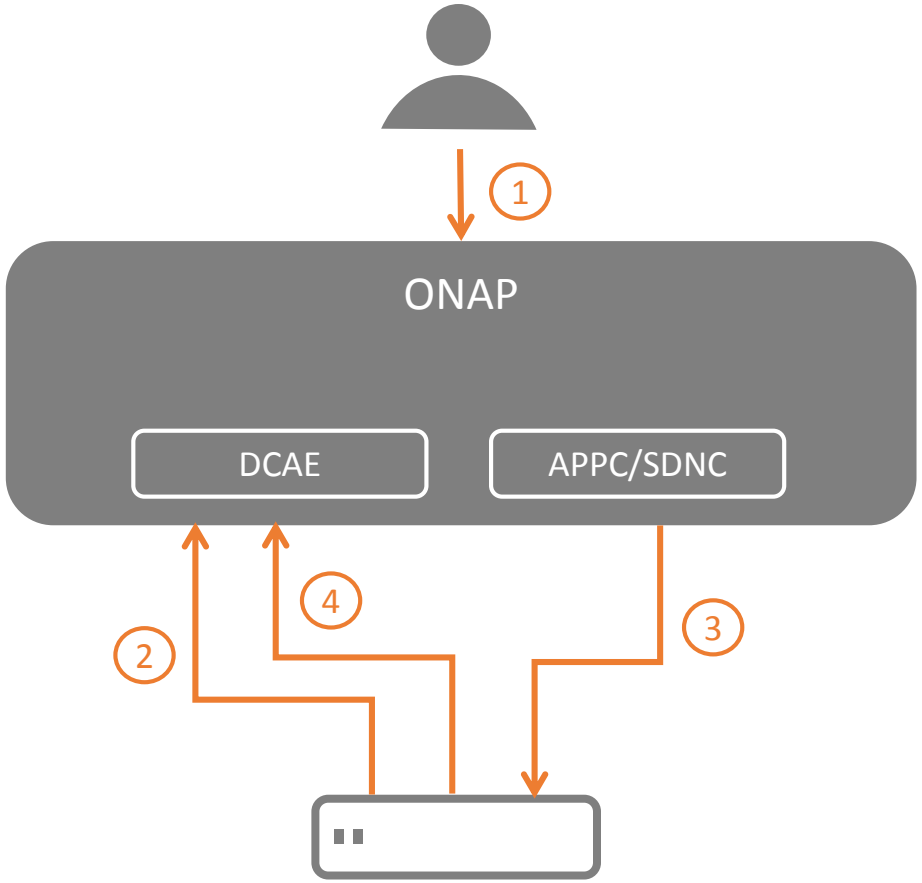
- Introduction of NFV means that VNFs deployed on shared infrastructure is quickly replacing dedicated physical equipment for many applications
- But some use cases still include PNFs as part of the E2E service, typically at the network edge
  - vCPE UC in ONAP R1
  - 5G RAN UC proposed for ONAP R2
- To achieve the full benefits of unified management and automation capabilities, native support for PNFs should be added in ONAP
  - Some support already exists today in R1
  - This presentation proposes some principles and highlights areas that need further discussion





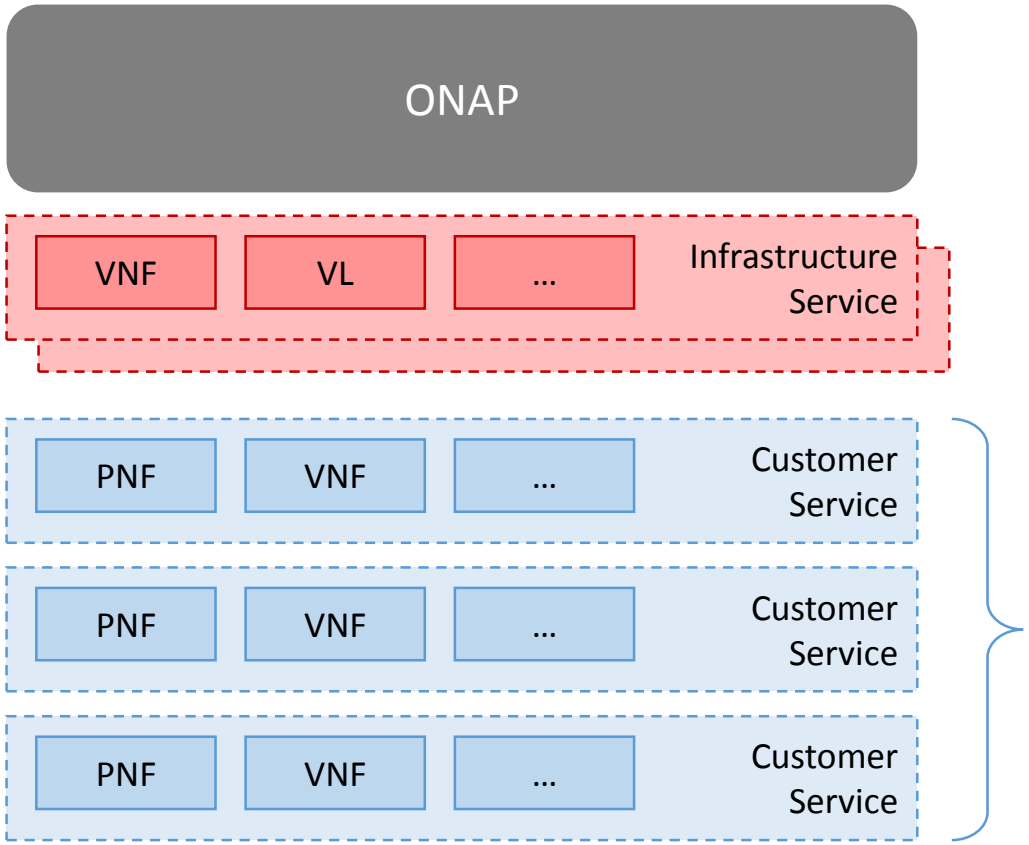
R2 PNF requirements

- The following requirement candidates are derived from the 5G RAN UC
  - Support for PNF Onboarding
    - Design & Orchestration (1)
    - Plug and Play (2)
  - Support for PNF Configuration (3)
    - Needs PNF IP address from (2)
  - Support for PNF Data Collection (4)
    - Needs configuration support from (3)
- Some of the flows such as PnP may depend on additional network functions not shown in this figure



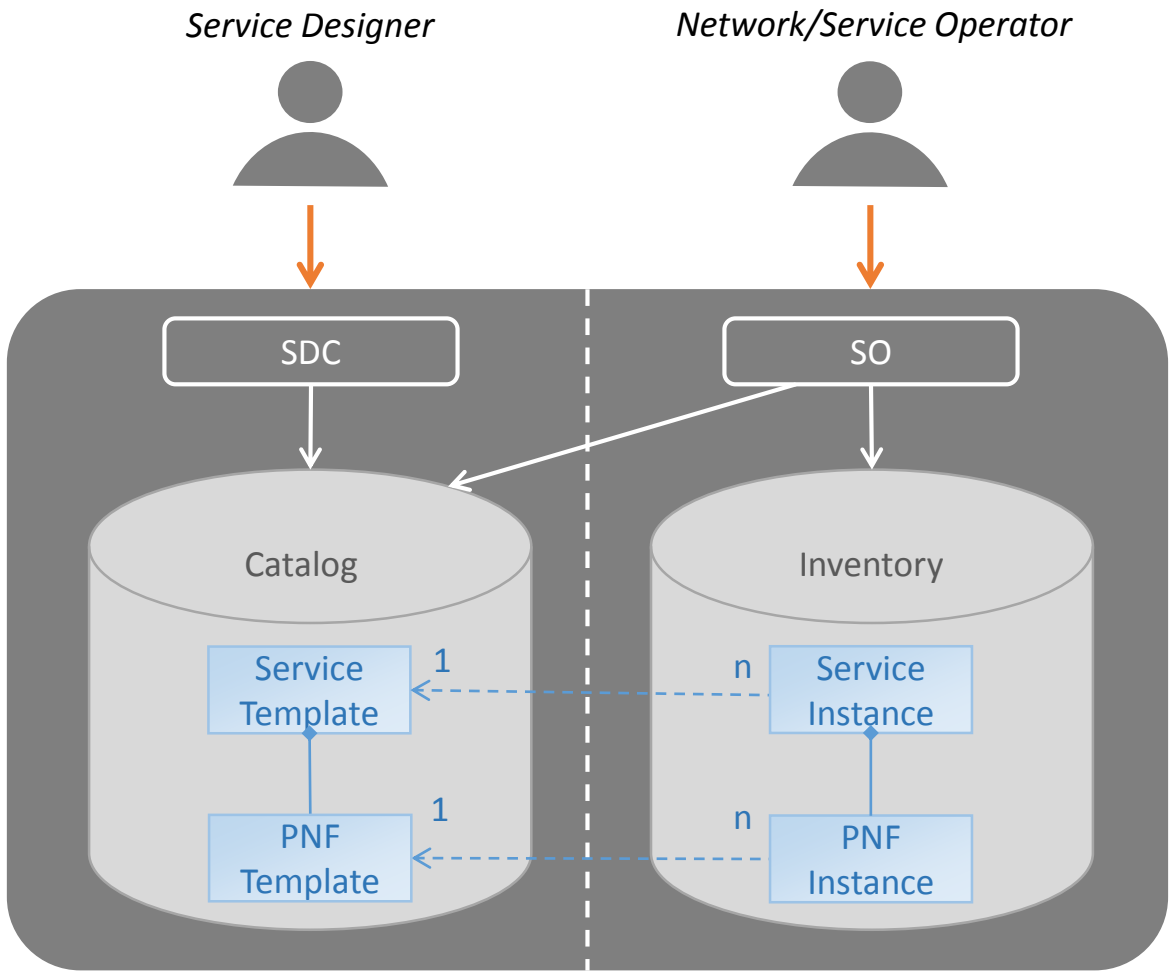
Use case service design pattern

- Two main classes of services
  - *Infrastructure services* provide resources for the UC supporting an entire network or area
  - *Customer services* are instantiated once per customer to allocate dedicated resources
    - These may include PNFs
- For the 5G RAN UC, all services are in principle infrastructure services
  - But gNBs share the same requirements as customer services for highly automated and large scale roll-out



Design-time and run-time entities

- Large scale roll-out requires template re-use
  - *Design once, instantiate multiple times*
- This principle must be supported also when service templates include PNFs
  - Corresponds to run-time binding of PNF nodes in the service topology to specific HW resource



Run-time binding using TOSCA

The service designer creates a service template where PNF serial number is an input parameter

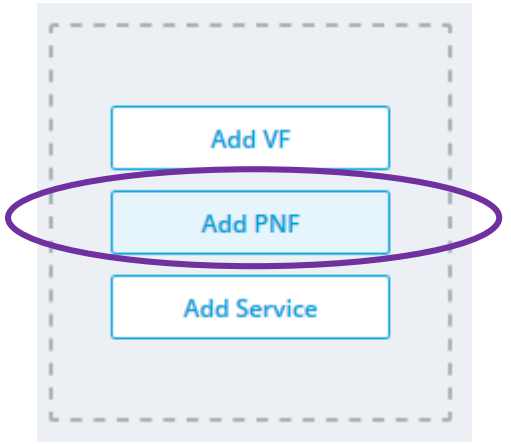
```
topology_template:
  inputs:
    serial_number:
      type: string
  node_templates:
    EdgeDevice:
      type: org.onap.resource.pnf.VendorAndModel
      properties:
        device_key: { get_input: serial_number }
```

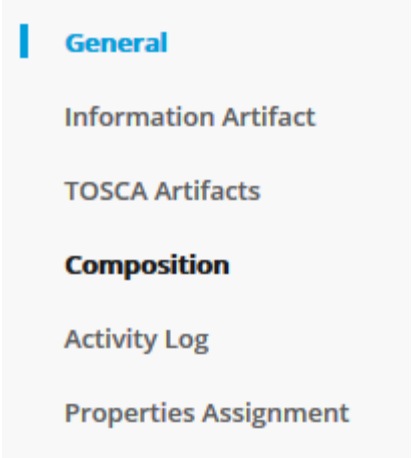
The network/service operator supplies the serial number when instantiating the service template

- There should be some flexibility when designing the service
  - Different parameters (serial number, MAC address etc) could be used for correlation depending on PNF type and the supported plug and play procedure
- Using an input parameter allows the service designer to declare what information must be provided when instantiating the service
  - But not fully in line with principle to avoid run-time attributes in the design-time model

PNF design model

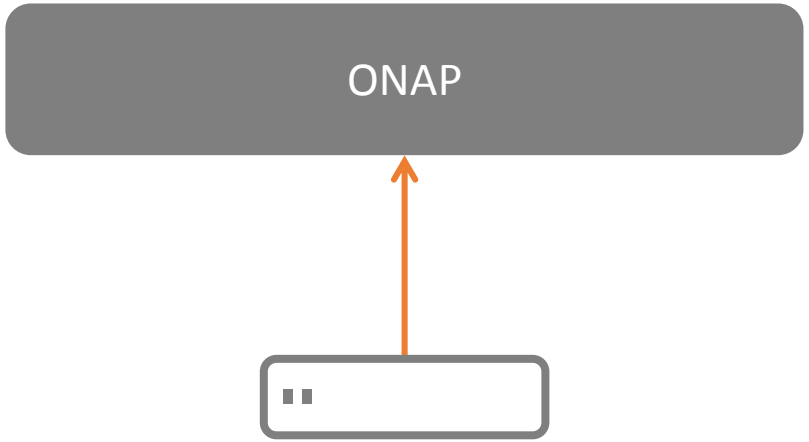
- New PNF types can be created in SDC, but what are catalog entries supposed to capture in their definition?
  - Do they have an internal composition, and what resources would be applicable for PNFs?
    - VNFs (VFs) are built up from VDUs, VLs, CPs etc
  - Is there any information that should be possible to import by onboarding vendor supplied data and artifacts?
    - VNF descriptors specify SW images





PNF Plug and Play requirements

- ONAP Plug and Play for PNFs should support
  - Providing the PNF with initial configuration and SW image if required
    - This step sets up the HW device so that further management via ONAP is possible, including application level configuration
  - Updating the PNF instance status in the inventory (AAI) when the PNF is detected
    - Register the PNF management IP address in case it is dynamically allocated from pool
- Security aspects must also be considered



PNF Plug and Play procedures

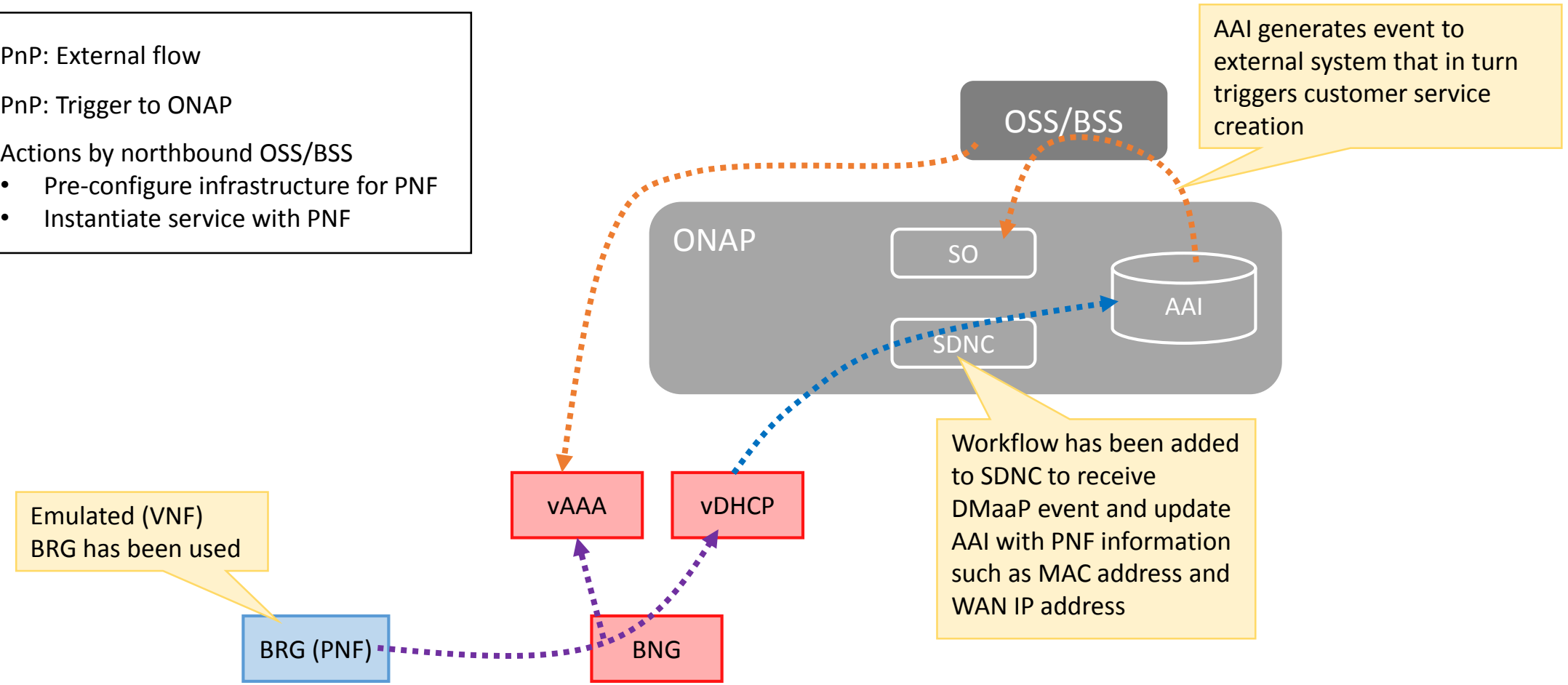
- On the following slides three examples are shown
  - vCPE UC from R1
  - Network scenario based on 3GPP TS 32.508 (Procedure flows for multi-vendor PnP)
    - While used here as example, the alignment of the 3GPP management architecture and ONAP is currently not settled
  - Network scenario based on draft-ietf-netconf-zerotouch mentioned in the proposed SD-WAN UC
    - Not approved as RFC by IETF yet
- As a platform, ONAP should be able to support several different PnP procedures!

Plug and Play – vCPE UC

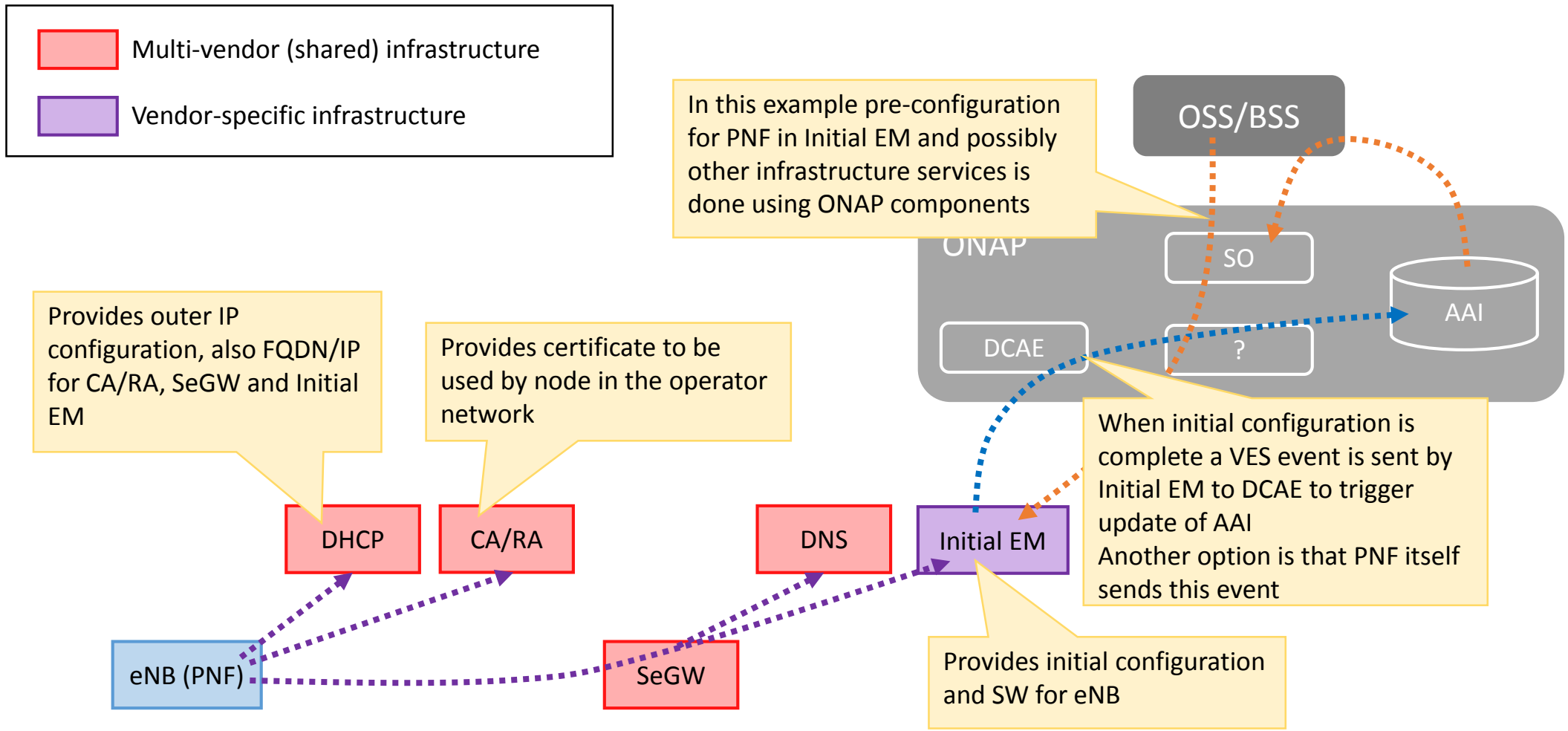
PnP: External flow

PnP: Trigger to ONAP

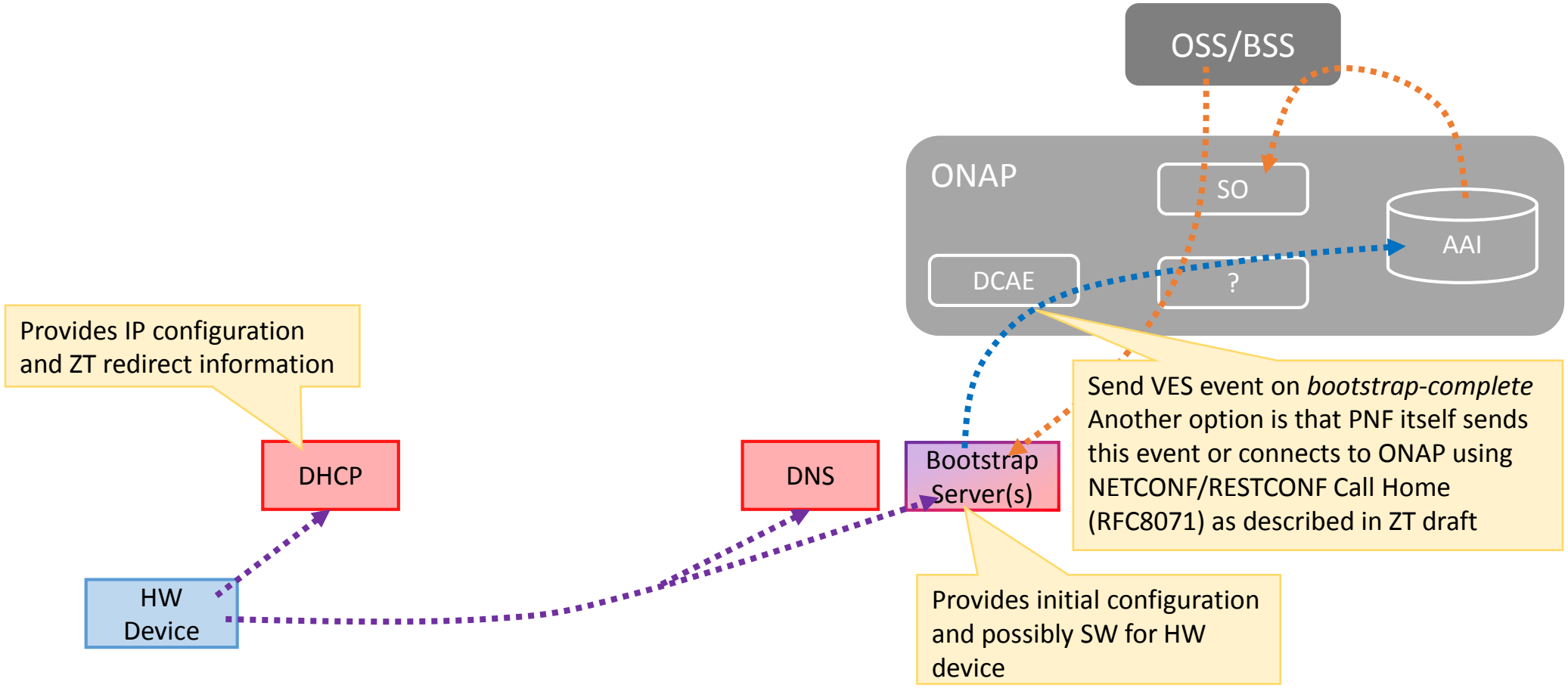
Actions by northbound OSS/BSS
- Pre-configure infrastructure for PNF
- Instantiate service with PNF



Plug and Play – Example derived from TS 32.508



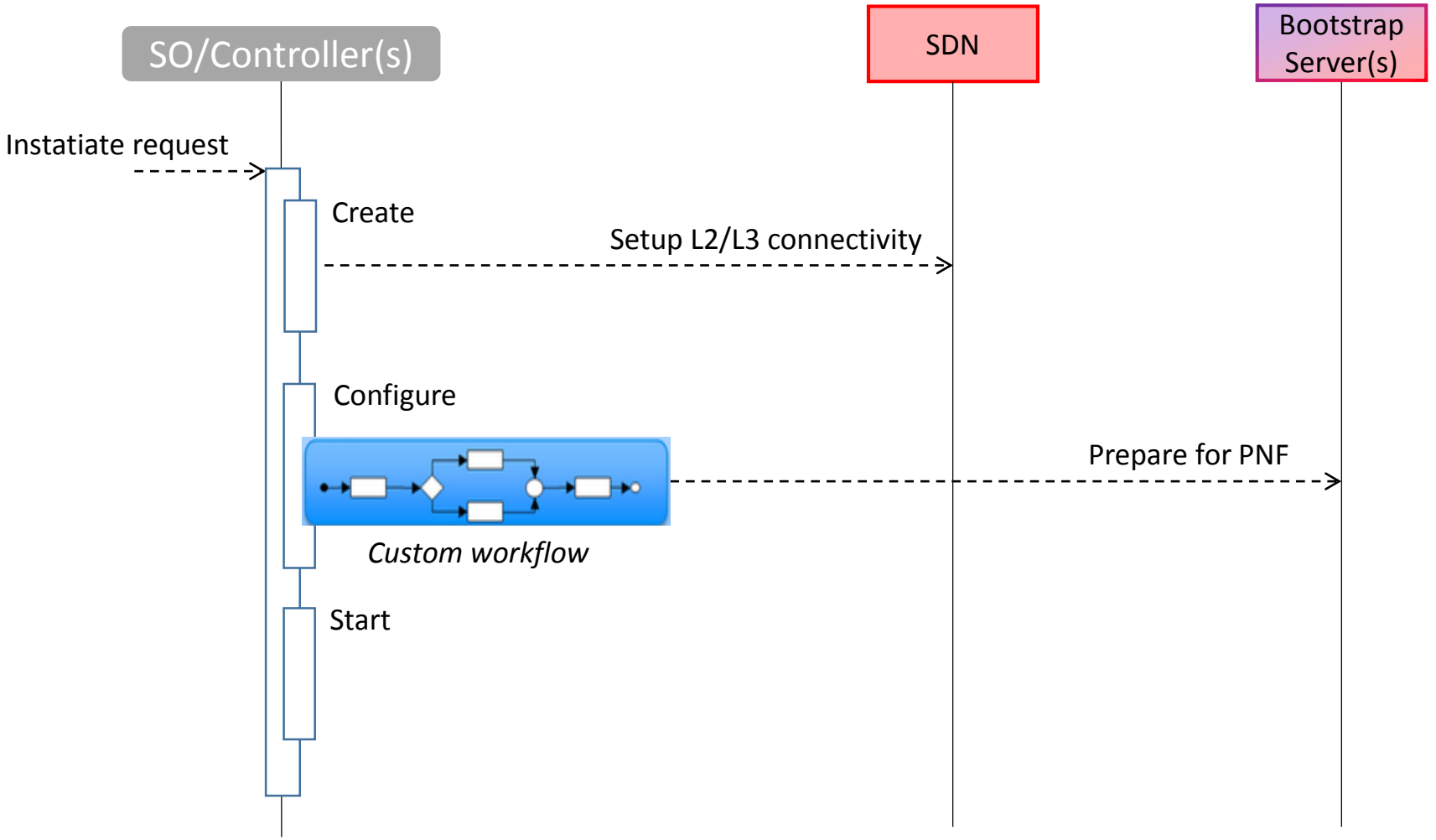
Plug and Play – Example derived from netconf-zerotouch



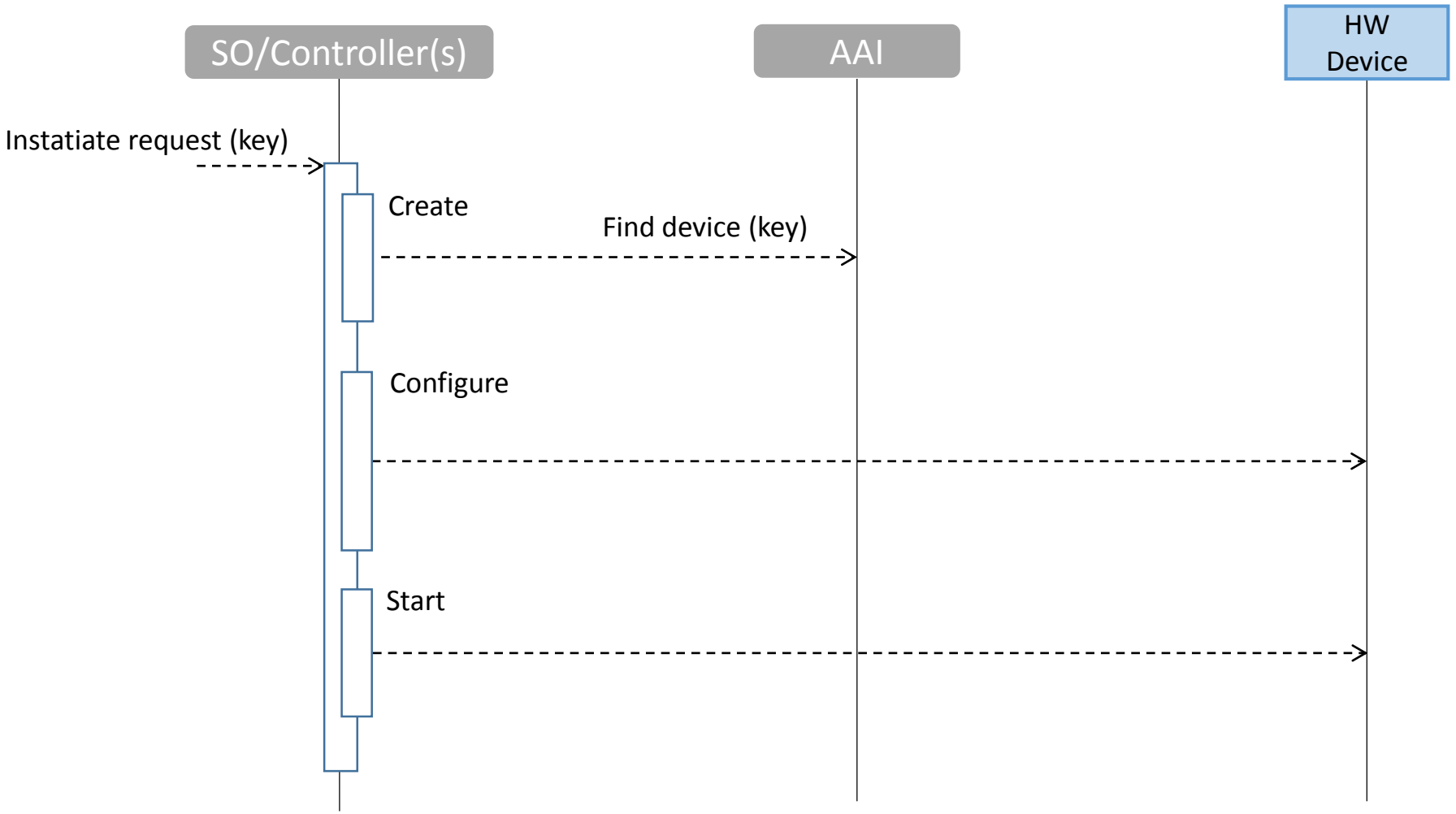
PNF Plug and Play security aspects

- PnP examples send events to ONAP in order to update AAI with information about the PNF
  - Call Home option (RFC8071) from ZT example would work in a somewhat different way
- The inventory update may in turn trigger further actions inside or outside ONAP
- For security reasons, it is important to ensure
  - The event source is authenticated
  - The inventory update is connected to policy deciding if operation is allowed for this event source
    - No matching policy – ignore PnP events from this event source (log as security incident?)
    - Policy allowing event source to register itself (event sent by PNF)
    - Policy allowing event source to act on behalf of other PNFs (e g DHCP server)
      - Event record must distinguish between event source and target PNF

Orchestration – PNF pre-configuration (optional)



Orchestration – Service with PNF



Orchestration and PnP issues

- What is the preferred work division between SO and controllers for the TOSCA standard lifecycle operations (create, configure, start)?
  - Execution of workflows
  - Update of inventory
- What controllers are involved in the different steps?
  - Orchestration
  - Handling PnP event from external system or device

Thank You